Dieser Standard richtet sich gleichermaßen wertschätzend an alle Personen (m/w/d). Zur besseren Lesbarkeit und Verständlichkeit des vorliegenden Standards wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern die männliche Form verwendet.

Anweisung/Kommunikation				
Aktivität	**OE**	**Name**	**Datum**	**Freigabe**
Einrichten	Group Cyber Security (CHV-C)	Governance & Risk Team Cyber Security	01.07.2023	per E-Mail
Fachliche Freigabe/ Anweisung	Group Cyber Security (CHV-C)	CISO	25.07.2023	per E-Mail
	Beschaffung (OFP)	Head of Procurement	25.07.2023	per E-Mail

Inhalt

Tabellenverzeichnis

1 Änderungen

Datum	**Änderung** (letzte 10 Änderungen)	**Autor** (Vorname, Name, OE)
24.04.2024	Informationsklassifizierung auf „öffentlich“ geändert.	AB, HS (CHV-CG)

2 Ziel

Ziel der Cybersicherheit ist der Schutz aller materiellen und immateriellen Vermögensgegenstände sowie der Mitarbeiter. Unternehmensinformationen – und auch die Systeme, die diese Informationen verarbeiten, – gelten bei RWE als besonders schützenswert. Deshalb ist Cybersicherheit Teil der umfassenden Sicherheitsstrategie von RWE und soll die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und IT-Systemen gewährleisten.

Die zunehmende Digitalisierung und Vernetzung von Unternehmen erfordert den Aufbau von Lieferketten und den Einsatz von Dienstleistern. Dies bringt neben vielen Vorteilen auch gewisse Risiken mit sich, die es im Rahmen eines ganzheitlichen Risikomanagements zu erkennen, bestmöglich abzuschwächen und zu verfolgen gilt.

Dieser Standard enthält Cybersicherheitsanforderungen, die von allen RWE-Partnern und -Anbietern sowie deren Unterauftragnehmern erfüllt werden müssen.

3 Anwendungsbereich

Dieser Standard gilt für alle Partner, Anbieter, Lieferanten und Dienstleiser der RWE AG und aller Konzerngesellschaften (einzeln und gemeinsam als „RWE“ bezeichnet). Es liegt in der Verantwortung der Partner, Anbieter, Lieferanten und Dienstleiser (nachstehend nur als Anbieter bezeichnet), die Sicherheitsanforderungen dieses Standards an alle ihre Unterauftragnehmer weiterzugeben.

Eine Ausnahme von diesem Standard besteht für Anbieter, die ausschließlich an Geräten von RWE arbeiten. Diese Anbieter müssen die folgenden Anforderungen nicht umsetzen, aber sie müssen sich an die Konzernfachregelung „GBR 002 Cybersicherheit – Mindeststandards für Mitarbeiter“ halten. Darüber hinaus können für den Bereich Operational Technology (OT) andere Regelungen gelten. Der Anforderer wird den betroffenen Anbietern diesen Standard zur Verfügung stellen. Der Anbieter ist dafür verantwortlich, sein Personal bezüglich der Einhaltung des genannten Dokuments anzuweisen.

Sämtliche Sicherheitsmaßnahmen werden auf der Grundlage der geltenden Gesetze und der aktuellen Rechtsprechung, einschließlich Mitbestimmungsrechten, durchgeführt, wobei gegebenenfalls verschiedene Zuständigkeiten zu berücksichtigen sind.

4 Anforderungen

Die Anforderungen werden im Folgenden definiert. Alle Anforderungen werden auf der Grundlage gängiger Cybersicherheitsstandards wie der ISO/IEC 27001 (2022) durchgeführt. Die Anforderungen unterscheiden sich in „Muss"- und „Sollte"-Anforderungen. „Muss"-Anforderungen müssen von allen RWE-Anbietern und ihren Unterauftragnehmern umgesetzt werden. „Sollte"-Anforderungen sind Empfehlungen und müssen nicht zwingend umgesetzt werden.

4.1 Organisation, Richtlinien und Verfahren der Informationssicherheit

Der Anbieter muss eine klare Organisation sowie entsprechende Richtlinien und Verfahren für die Informationssicherheit einrichten, um potenzielle Sicherheitsrisiken zu minimieren.

- Der Anbieter muss für ein effektives Sicherheitsmanagement klare Rollen, Zuständigkeiten und Verantwortlichkeiten im Bereich der Informationssicherheit festlegen. Je nach Größe und Umfang der Verantwortlichkeiten muss der Anbieter mindestens einen Sicherheitsbeauftragten ernennen, der bzw. die über die erforderlichen Kenntnisse, Erfahrungen und Befugnisse verfügt/verfügen, um die Informationssicherheit im Unternehmen zu überwachen und sicherzustellen, dass die Sicherheitsvorschriften und -verfahren koordiniert und kontrolliert werden.
- Der Anbieter muss schriftliche Informationssicherheitsrichtlinien erstellen, aufrechterhalten und durchsetzen, die von der Geschäftsleitung genehmigt und den Mitarbeitern mitgeteilt werden. Diese müssen ihre Verpflichtungen zum Schutz vertraulicher Informationen und zur akzeptablen Nutzung aller Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung gegenüber RWE relevant sind, verstehen. Die Informationssicherheitsrichtlinien sollten mindestens einmal jährlich überprüft und gegebenenfalls aktualisiert werden, um ihre Relevanz und Wirksamkeit zu gewährleisten.
- Der Anbieter muss über Verfahren zur Verwaltung seiner an der Leistungserbringung beteiligten Unterauftragnehmer verfügen, die ihre Fähigkeit zur Einhaltung der Sicherheitskontrollstandards schriftlich bestätigen müssen.
- Der Anbieter sollte ein genaues, aktuelles Bestandsverzeichnis aller Vermögenswerte (Assets) und Informationsverarbeitungsstandorte führen, die für die Leistungserbringung gegenüber RWE genutzt werden, einschließlich der verantwortlichen Eigentümer der Vermögenswerte (Assets).

4.2 Sicherheit im Bereich Personal/Human Resources (HR)

Der Anbieter muss HR-Verfahren und -Prozesse implementiert haben, die alle an der Leistungserbringung für RWE beteiligten Personen einbeziehen, um mögliche Sicherheitsrisiken zu minimieren.

- Der Anbieter muss bei allen Mitarbeitern (einschließlich Auftragnehmern und Zeitarbeitskräften), die an der Leistungserbringung gegenüber RWE beteiligt sind, eine Hintergrundüberprüfung oder ein Einstellungsscreening durchführen. Die Überprüfungen oder Screenings sollten den kriminellen und beruflichen Hintergrund der Mitarbeiter umfassen. Der Grad der Überprüfung muss in einem angemessenen Verhältnis zur Kritikalität und zum Risiko stehen, die mit der Rolle oder Aufgabe innerhalb der Organisation verbunden sind, und mit geltendem Recht vereinbar sein.
- Der Anbieter sollte sicherstellen, dass das Personal des Anbieters, bevor es seine Arbeit für RWE aufnimmt, die für die jeweilige Rolle erforderliche Ausbildung und Schulung im Bereich der Informationssicherheit (nachweislich) abgeschlossen hat. Ein umfassendes Programm zur Förderung des Sicherheitsbewusstseins des gesamten Personals, das die Ausbildung, Schulung und Aktualisierung der Sicherheitsrichtlinien, -verfahren und -anforderungen umfasst, ist obligatorisch. Entsprechende Schulungen sollten regelmäßig wiederholt und durch geeignete Aktivitäten und Materialien verstärkt werden.
- Das Personal des Anbieters sollte Geheimhaltungs- oder Vertraulichkeitsvereinbarungen unterzeichnen, bevor es Zugang zu Informationen und anderen zugehörigen Vermögenswerten (Assets) sowie zu Einrichtungen im Zusammenhang mit den für RWE erbrachten Dienstleistungen erhält. Darüber hinaus muss sich das Personal des Anbieters schriftlich verpflichten, die Sicherheitsanforderungen und Organisationsrichtlinien des Anbieters einzuhalten.
- Der Anbieter sollte über formalisierte und kommunizierte Disziplinarverfahren verfügen, um gegen Mitarbeiter vorzugehen, die gegen die Sicherheitsrichtlinien und -verfahren des Anbieters verstoßen, wobei Maßnahmen in Abhängigkeit von der Art und Schwere des Verstoßes festzulegen sind.
- Der Anbieter muss Prozesse und Verfahren für Einsteiger/Aussteiger/Umsteiger einrichten, um z. B. den Zugang in Verbindung mit den Kapiteln 4.6.9 Kontoverwaltung und 4.6.10 Identitäts- und Zugriffsverwaltung zu verwalten.

4.3 Umgang mit und Meldung von Sicherheitsvorfällen

Der Anbieter muss Verfahren für Sicherheitsvorfälle implementiert haben, die ein effektives und geordnetes Management von Sicherheitsvorfällen für Prozesse ermöglichen, die für die Leistungserbringung gegenüber RWE relevant sind.

- Diese Verfahren müssen dokumentiert werden und sollten die Überwachung, Erkennung, Klassifizierung, Analyse und Meldung sowie die Reaktion auf und Lösung von Sicherheitsvorfällen abdecken und die damit verbundenen Rollen und Verantwortlichkeiten festlegen. Darüber hinaus müssen für jeden Sicherheitsvorfall, der sich auf RWE Vermögenswerte (Assets) auswirkt, eine Ursachenanalyse sowie Verfahren im Zusammenhang mit gewonnenen Erkenntnissen durchgeführt werden.
- Gemeldete Sicherheitsvorfälle müssen überprüft und anschließend analysiert werden, um zu ermitteln, wie sie sich auswirken.
- Alle bestätigten Sicherheitsvorfälle müssen klassifiziert, nach Prioritäten geordnet und dokumentiert werden.
- Sicherheitsvorfälle müssen von Mitarbeitern bearbeitet werden, die in der Bearbeitung und Bewertung von Sicherheitsvorfällen geschult sind (z.B. ein spezielles Reaktionsteam für Sicherheitsvorfälle).
- Sämtliche Aktivitäten zum Vorfallmanagement müssen protokolliert werden, und die Protokolle müssen manipulationssicher sein.
- Der Anbieter muss RWE alle ihm bekannt gewordenen Sicherheitsvorfälle, Ereignisse und/oder Schwachstellen, die RWE betreffen oder beeinträchtigen, unverzüglich (spätestens jedoch innerhalb von 24 Stunden) per E-Mail (csirt@rwe.com) melden.

4.4 Umgang mit Informationen

Informationen sind ein wichtiges Gut für RWE und müssen über den gesamten Informationslebenszyklus zu jedem Zeitpunkt angemessen geschützt werden. Dies gilt von der Erstellung der Informationen über deren Aufzeichnung und Löschung bis hin zur Entsorgung. Daher sind die folgenden Maßnahmen auch von allen Anbietern umzusetzen, um einen vollständigen Schutz der Informationen von RWE zu erreichen.

- Der Anbieter sollte ein Verzeichnis der Informationen und anderer zugehöriger Vermögenswerte (Assets) von RWE, einschließlich der jeweiligen Verantwortlichen, führen.

Der Anbieter muss Regelungen für den Umgang mit Informationen umsetzen:

- Der Anbieter muss über Clear-Screen- und Clean-Desk-Vorschriften verfügen, um sicherzustellen, dass Unbefugte an den Arbeitsplätzen keinen Zugang zu Informationen haben.
- Es sollten Regelungen für eine sichere Kommunikation (Nutzung von E-Mails und Messengern) getroffen werden.
- Der Anbieter sollte Kommunikationsmittel für die Übermittlung von Geschäftsinformationen festlegen und genehmigen.

Werden sensible Informationen von RWE durch den Anbieter verarbeitet, müssen folgende zusätzliche Maßnahmen umgesetzt werden:

- Es sollten Vorschriften für die Vernichtung/Entsorgung von Informationen am Ende ihres Lebenszyklus festgelegt werden. Für die Vernichtung von „vertraulichen“ und „streng vertraulichen“ RWE-Informationen muss ein Schredder/Aktenvernichter verwendet werden.
- E-Mails mit sensiblen RWE-Informationen sollten auf jeden Fall verschlüsselt werden (siehe Kapitel 4.6.7 Verschlüsselung).
- Medien mit vertraulichen Informationen von RWE müssen unter Verschluss gehalten werden.
- Für die dauerhafte Aufbewahrung von Medien, die streng vertrauliche RWE-Informationen enthalten, ist eine geeignete Aufbewahrungsmöglichkeit (z.B. Tresor oder Stahlschrank) zu nutzen. Medien, die streng vertrauliche RWE-Informationen enthalten, sind im täglichen Gebrauch mit den vorhandenen technischen Möglichkeiten so weit wie möglich unter Verschluss zu halten.

4.4.1 Klassifizierung und Kennzeichnung

Die Vorgaben zur Klassifizierung und Kennzeichnung von Informationen basieren auf den internen Regelungen von RWE. Die Anforderungen sind auch vom Anbieter umzusetzen, um durch ein einheitliches Vorgehen einen ganzheitlichen Schutz der Informationen von RWE zu erreichen. Sämtliche Informationen (von RWE und seinen Kunden) müssen von RWE-Anbietern und deren Unterauftragnehmern gemäß diesen Anforderungen und gegebenenfalls zusätzlich zum Vertrag beigefügten Regelungen zum Umgang mit Informationen geschützt werden.

- Sämtliche Informationen, die sich auf die Leistungserbringung gegenüber RWE beziehen, müssen klassifiziert und gemäß den vorgegebenen Anforderungen gekennzeichnet werden (siehe Anhang 1: Klassifizierung und Kennzeichnung von Informationen).

4.5 Schutz vor physischem Zutritt und Umwelteinflüssen

Die Räumlichkeiten/Einrichtungen, die für die Leistungserbringung gegenüber RWE relevant sind, müssen ordnungsgemäß geschützt werden, um unbefugten physischen Zugang zu verhindern. Daher muss der Anbieter die folgenden Maßnahmen ergreifen:

- Physische Schutzmaßnahmen (Zäune, physische Barrieren, Sicherheitspersonal, Einbruchmeldeanlagen, Videoüberwachungssysteme usw.) müssen entsprechend den Anforderungen beurteilt und für die Umsetzung ausgewählt werden, die in Bezug auf die Vermögenswerte (Assets) in den Räumlichkeiten/Einrichtungen gelten. Der Umfang der angewandten Maßnahmen sollte immer im Verhältnis zur Kritikalität der in den Einrichtungen gelagerten Geräte und Systeme und zum Risiko für den Geschäftsbetrieb, das sich aus der Beeinträchtigung oder Zerstörung dieser Geräte und Systeme ergibt, stehen.
- Der physische Zugang muss auf die Personen beschränkt werden, die ihn geschäftlich benötigen, und sollte entsprechend dokumentiert und durch geeignete Maßnahmen geschützt werden. Es sollten Authentifizierungsmechanismen, z.B. Zugangskarten, vorhanden sein.
- Ein dokumentierter Prozess für die Zugangsverwaltung ist erforderlich und muss die Beantragung von Zugangsrechten, eine regelmäßige Überprüfung und den Widerruf von Berechtigungen umfassen.
- Der Zugang Dritter zu den betreffenden Informationsverarbeitungsvorrichtungen muss streng kontrolliert, dokumentiert und auf ein Minimum beschränkt werden.

Werden sensible RWE-Informationen durch den Anbieter verarbeitet, müssen folgende zusätzliche Maßnahmen umgesetzt werden:

- Der physische Zugang zu Räumlichkeiten/Einrichtungen, in denen sensible RWE-Informationen verarbeitet werden, muss durch geeignete physische Zugangsmaßnahmen (z.B. Drehkreuze oder Schleusen) geschützt werden, um das (beabsichtigte oder unbeabsichtigte) Einschleusen unbefugter Personen durch autorisierte Personen („Piggybacking“) zu verhindern. In jedem Fall muss der physische Zugang so gestaltet sein, dass jeweils nur eine Person Zugang zu den zugangsbeschränkten Bereichen hat.
- Wenn das Personal des Anbieters auf derselben Etage innerhalb eines Gebäudes/einer Einrichtung an anderen Aufträgen arbeitet (d.h. für andere Unternehmen als RWE), müssen für die für RWE erbrachten Leistungen eigene Arbeitsbereiche eingerichtet werden. Diese Räume/Bereiche müssen (mindestens) durch organisatorische Kontrollen wie spezielle Schilder und Sensibilisierungskampagnen für Mitarbeiter geschützt werden, um den Informationsschutz zu gewährleisten und das Risiko eines unbefugten Zugangs zu dem spezifischen Bereich, in dem sensible RWE-Daten verarbeitet werden, zu verringern.

Die Räumlichkeiten/Einrichtungen, die für die Leistungserbringung gegenüber RWE relevant sind, müssen ordnungsgemäß geschützt werden, um Schäden durch physische und umgebungsbedingte Bedrohungen zu verhindern. Daher muss der Anbieter die folgenden Maßnahmen ergreifen:

- Die entsprechenden Maßnahmen zum Schutz vor physischen und umweltbedingten Bedrohungen (z. B. Feuer, Überschwemmungen, Überspannungen) sollten angemessen sein und der Bedeutung der Gebäude und der Kritikalität der in diesen Gebäuden durchgeführten Betriebsabläufe oder der dort befindlichen IT-Systeme im Hinblick auf die Leistungserbringung gegenüber RWE entsprechen. Die Einrichtungen müssen über geeignete Schutzmaßnahmen zur frühzeitigen Erkennung von Rauch, Feuer, Feuchtigkeit und Wasser in der Einrichtung verfügen.

4.6 Sicherheitsanforderungen für den IT-Betrieb

4.6.1 Management technischer Schwachstellen und Patch-Management

Der Anbieter sollte einen umfassenden und dokumentierten Schwachstellen- und Patch-Management-Prozess für alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte implementieren, die für die Leistungserbringung gegenüber RWE relevant sind, um Angriffe zu reduzieren und potenzielle Sicherheitsrisiken zu minimieren. Angreifer suchen ständig nach neuen Angriffsmethoden oder Schwachstellen in bestehenden Diensten. Daher ist es wichtig, dass Software und Hardware regelmäßig auf Schwachstellen überprüft und vorhandene Updates und Patches eingespielt werden.

Identifikation von Schwachstellen:

- Der Anbieter sollte Informationen von Software- und Hardwareanbietern (die für die Leistungserbringung gegenüber RWE relevant sind) und anderen relevanten Quellen in Bezug auf technische Schwachstellen nachverfolgen. Darüber hinaus muss der Anbieter regelmäßig Schwachstellen-Scans durchführen und die Gefährdung durch entdeckte Schwachstellen umgehend beurteilen, um sicherzustellen, dass geeignete Maßnahmen zur Behebung potenzieller Risiken ergriffen werden.
- Schwachstellen müssen nach einem anerkannten Industriestandard mit einem Schweregrad bewertet werden, z.B. nach dem Common Vulnerability Scoring System (CVSS Score, allgemeines Bewertungssystem für Schwachstellen). Darüber hinaus sollten Schwachstellen entsprechend der zugewiesenen Kritikalität zeitnah behoben werden.

Umgang mit festgestellten Schwachstellen:

- Der Anbieter muss sicherstellen, dass im Zusammenhang mit entdeckten Schwachstellen (die für die Leistungserbringung gegenüber RWE relevant sind) entweder ein entsprechender Software-Patch angewendet wird, um die Schwachstellen zu beheben, ODER dass Schwachstellen nach einem formalisierten und dokumentierten, vom verantwortlichen Management genehmigten Risikobehandlungsplan behoben werden, um das Risiko der jeweiligen Schwachstellen auf ein akzeptables Niveau zu reduzieren. Dies sollte entsprechend der zugewiesenen Kritikalität zeitnah geschehen.
- Relevante Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte sollten so konfiguriert werden, dass sie Software-Patches und andere relevante Updates automatisch von einem zentralen Verwaltungs- und Verteilungsdienst erhalten, sofern dies technisch machbar ist.

4.6.2 Änderungsmanagement

- Änderungen an Informationsverarbeitungseinrichtungen, Informationssystemen, Anwendungen, Plattformen, Infrastruktur und/oder den zugrunde liegenden physischen und technischen Räumlichkeiten, die für die Leistungserbringung gegenüber RWE relevant sind, müssen förmlichen Änderungsmanagementverfahren unterliegen, die dokumentiert und vom verantwortlichen Management des Anbieters genehmigt werden sollten. Der Anbieter sollte Aufzeichnungen über alle relevanten Änderungen führen, einschließlich Informationen zu Datum, Uhrzeit und Genehmigung der Änderungen.
- Änderungen, die möglicherweise Auswirkungen auf die vertraglich vereinbarten Leistungen haben, sind RWE durch den Anbieter in angemessener Zeit im Voraus mitzuteilen (per E-Mail an informationsecurity@rwe.com). Dies kann unter anderem umfassen, ist aber nicht beschränkt auf:
    - (umfangreiche) Änderungen der physischen Infrastruktur (z.B. Umzug in eine andere Einrichtung oder ein anderes Gebäude/eine andere Etage) sowie der technischen Infrastruktur (z. B. größere Upgrades von Betriebssystemen und/oder Anwendungen oder erhebliche Neukonfiguration von Systemen und/oder Diensten)
    - Verlagerung der physischen und/oder technischen Infrastruktur in eine andere geografische Region oder einen anderen Rechtsraum
    - Verarbeitung von Informationen in einem neuen geografischen oder rechtlichen Gebiet

4.6.3 Endpunkt-/Gerätesicherheit

Sämtliche Anbieterressourcen, die für die Leistungserbringung gegenüber RWE relevant sind, sollten einem Endpunktschutz, Malwarekontrollen und Kontrollen der Installation von Endbenutzersoftware unterliegen, um die Angriffsfläche zu verringern und potenzielle Sicherheitsrisiken zu minimieren.

- Sämtliche Endpunkte sollten zentral verwaltet werden und über eine aktualisierte und ordnungsgemäß konfigurierte Endpunktschutzsoftware verfügen (einschließlich regelmäßiger Überprüfungen und Definitionsaktualisierungen), um die Verbreitung von Malware zu verhindern. Darüber hinaus müssen die Endpunkte mit aktuellen Sicherheits-Patches und Software-Updates auf dem neuesten Stand gehalten werden.
- Die Installation von Endbenutzersoftware bezieht sich auf den Prozess, der es Mitarbeitern erlaubt oder verwehrt, an ihren Arbeitsplätzen Software zu installieren. Durch nicht autorisierte Software-Installationen können dem Unternehmensnetzwerk Schwachstellen und Malware hinzugefügt werden.
    - Die Installation von Software auf Geräten, die im Besitz des Anbieters sind, sollte entsprechend verwaltet werden (z.B. mithilfe einer Whitelist oder Blacklist).
    - Die gesamte Software, die auf Geräten des Anbieters installiert ist, muss lizenziert und ordnungsgemäß gewartet werden, um Sicherheit und Konformität zu gewährleisten. Dazu gehört es, alle Softwareversionen im Auge zu behalten und die erforderlichen Updates und Patches anzuwenden.

4.6.4 Härtung

Der Anbieter muss alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung gegenüber RWE relevant sind, härten, um Angriffe zu reduzieren und potenzielle Sicherheitsrisiken zu minimieren.

- Die Härtung sollte vor dem Einsatz in der Produktion erfolgen, einschließlich der Behebung bekannter Schwachstellen und der Implementierung eines sicheren Basisplans oder der Verwendung sicherer Baseline-Builds.
- Alle allgemeinen, Gast-, Wartungs- und Standardkonten sollten deaktiviert werden.
- Die Festplattenverschlüsselung sollte aktiviert sein.
- USB-Anschlüsse sollten nach Möglichkeit deaktiviert werden.
- Konfigurationsbereiche (z.B. BIOS, EFO, Windows-Systemsteuerung) sollten für normale Benutzer nicht zugänglich/veränderbar sein.

- Sämtliche Standardpasswörter müssen änderbar sein und in einen individuellen, nicht standardisierten Wert geändert werden (siehe 4.6.11, „Passwortverwaltung“).

4.6.5 Sichere Entwicklung

Der folgende Abschnitt betrifft ausschließlich Anbieter, die im Rahmen der Softwareentwicklung für RWE tätig sind.

- Die Entwicklung von Software muss dem Stand der Technik entsprechende Sicherheitsanforderungen erfüllen und einem gemeinsamen Sicherheitsrahmen bzw. einem gemeinsamen sicheren Softwareentwicklungszyklus (S-SDLC) folgen, z.B. OWASP. Für das zu entwickelnde Projekt sollten je nach Kritikalität und Verwendungszweck geeignete zusätzliche Maßnahmen und Anforderungen entwickelt und erfüllt werden.
- Es sollte eine Entwicklungspipeline oder ein Staging-Prozess eingerichtet werden, um sicherzustellen, dass nur getestete und genehmigte Änderungen in den Produktivsystemen implementiert werden. Dies umfasst sowohl Funktionalitäts- als auch Sicherheitsaspekte und sollte Qualitätsprüfungen wie Software-Code-Scanner und Peer-Reviews beinhalten.
- Der Anbieter muss alle festgestellten Sicherheitsprobleme vor der Lieferung beheben. Bei Sicherheitsproblemen, die nach der Lieferung entdeckt oder begründet vermutet werden, sollte RWE bei der Durchführung einer Untersuchung, bei der das Problem bestimmt wird, sowie bei dessen Behebung in einem angemessenen Zeitrahmen in Bezug auf das damit verbundene Risiko unterstützt werden.
- Eine verständliche Dokumentation sollte in Übereinstimmung mit den Anforderungen und Spezifikationen erstellt werden.

4.6.6 Netzwerk- und Architektursicherheit

Der Anbieter muss alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung gegenüber RWE relevant sind, schützen, um Angriffe zu reduzieren und potenzielle Sicherheitsrisiken zu minimieren. Der Schutz des Netzwerks und der Clients vor unbefugtem Zugriff, Missbrauch oder Diebstahl ist unerlässlich, um die Auswirkungen von Angriffen einzudämmen und ihre Ausbreitung zu verhindern. Die Netzwerksicherheit kombiniert mehrere Verteidigungsebenen an der Peripherie und im Netzwerk.

- Der Anbieter sollte eine geeignete Netzwerkarchitektur einrichten, die verschiedene Segmente umfasst, wobei jedes Segment einem bestimmten Zweck dient und nur die erforderlichen Systeme und Daten enthält. Dies trägt dazu bei, den Umfang eines potenziellen

Sicherheitsverstoßes zu begrenzen, und macht es einfacher, etwaige Probleme zu erkennen und einzudämmen.

- Insbesondere Netzwerke der Betriebstechnik (OT) und des industriellen Kontrollsystems (ICS) sollten mithilfe physisch getrennter Netzwerkgeräte logisch vom Unternehmensnetzwerk getrennt werden.
- Der Anbieter sollte geeignete Komponenten der Netzwerksicherheitsinfrastruktur wie Firewalls, Angriffserkennungs-/Angriffsverhinderungssysteme (IDS/IPS) und vergleichbare Sicherheitskontrollen implementieren. Diese Komponenten sollten regelmäßig gewartet werden. Die Firewall muss (sofern technisch möglich) so konfiguriert sein, dass sie alle bekannten Sicherheitslücken schließt.
- Der Anbieter muss den Fernzugriff auf sein Netzwerk genehmigen und auf autorisiertes Personal beschränken. Wenn ein Fernzugriff auf die Netzwerke und Clients des Anbieters erforderlich ist, müssen sichere und verschlüsselte Methoden wie virtuelle private Netze (VPNs) und MFA verwendet werden.
- Vorzugsweise sollten Anbieter über virtuelle Remote-Desktop-Technologie (VDI) auf RWE-Netzwerke und -Informationssysteme zugreifen.
- Der Anbieter muss Maßnahmen zur Sicherung seiner E-Mail-Systeme umsetzen. Dies kann die Verwendung von Spam-Filtern, E-Mail-Verschlüsselung und die Umsetzung von E-Mail-Richtlinien zur Verhinderung der Weitergabe sensibler Informationen umfassen.

4.6.7 Verschlüsselung

Der Anbieter muss sicherstellen, dass Verschlüsselungsmechanismen umgesetzt werden, um die unbefugte Offenlegung und Veränderung von Informationen, die für die Leistungserbringung gegenüber RWE relevant sind, zu verhindern.

- Der Einsatz von Verschlüsselungslösungen muss im Hinblick auf behördliche Vorschriften geprüft werden.
- Verschlüsselungslösungen sollten bewährte Verfahren für sichere Versionen und Konfigurationen berücksichtigen, die im Rahmen globaler Informationssicherheitsstandards (z.B. ENISA, FIPS, BSI usw.) verfügbar sind.
- Es sollte ein System zur Verwaltung kryptografischer Schlüssel vorhanden sein, das Verfahren für den gesamten Lebenszyklus der Schlüssel (von der Erzeugung bis zum Widerruf/zur Vernichtung) und Maßnahmen zu deren Schutz umfasst.

Werden sensible Informationen von RWE durch den Anbieter verarbeitet, müssen folgende zusätzliche Maßnahmen angewendet werden:

- Sensible Informationen von RWE (die als vertraulich und streng vertraulich eingestuft sind) müssen bei der Übertragung (in transit) und der Aufbewahrung (at rest) anhand genehmigter Verschlüsselungsalgorithmen mit angemessener Schlüssellänge und kryptografischer Stärke verschlüsselt werden.

4.6.8 Protokollierung und Überwachung

Der Anbieter muss alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung gegenüber RWE relevant sind, überwachen und entsprechende Ereignisprotokolle erstellen. Darüber hinaus müssen auch die physischen Zugangsmaßnahmen (z.B. Türen, Drehkreuze oder Schleusen) von Räumlichkeiten/Einrichtungen, in denen sensible RWE-Informationen verarbeitet werden, überwacht und entsprechende Protokolle erstellt werden, damit der physische Zugang jederzeit nachvollzogen werden kann.

- Ereignisprotokolle sollten so detailliert sein, dass sie bei der Ermittlung der Ursache eines Problems helfen und eine Rekonstruktion der Abfolge der Ereignisse ermöglichen. Dies umfasst, ist aber nicht beschränkt auf die Aufzeichnung von Datum, Uhrzeit und Quellort (IP-Adresse/Hostname) für alle Zugriffsversuche sowie die Erfassung von System- und Netzwerksicherheitsinformationen, Warnungen, Ausfällen, Ereignissen und Fehlern.
- Ereignisprotokolle müssen kontinuierlich überwacht und regelmäßig überprüft werden, um ungewöhnliche, verdächtige und/oder unbefugte Aktivitäten zu analysieren und zu identifizieren.
- Ereignisprotokolle sollten auf einem zentralen System (z.B. einem zentralen Protokollserver) gespeichert und konsolidiert werden, um die Integrität der Protokolldateien zu gewährleisten und sie vor Manipulationen zu schützen.
- Der Zugang zu den zentralen Systemen, in denen die Protokolldateien gespeichert werden, muss eingeschränkt werden. Benutzer, auch solche mit privilegierten Zugriffsrechten, sollten nicht die Erlaubnis erhalten, Protokolle ihrer eigenen Aktivitäten zu löschen oder zu deaktivieren, damit eine korrekte und unverfälschte Aufzeichnung der Ereignisse gewährleistet ist.

4.6.9 Kontoverwaltung

Der Anbieter muss über eine Kontoverwaltungslösung verfügen, um Informationen durch die kontrollierte Nutzung von Benutzerkonten, die für die Leistungserbringung gegenüber RWE relevant sind, zu schützen und dadurch mögliche Sicherheitsrisiken zu minimieren.

- Der Anbieter muss ein Verzeichnis aller Konten, die für die Leistungserbringung gegenüber RWE relevant sind, anlegen und pflegen.
- Der Anbieter muss auf den RWE zur Verfügung gestellten Systemen strenge Maßnahmen zur Kontoverwaltung einsetzen und das Prinzip der geringsten Privilegien anwenden.

4.6.10 Identitäts- und Zugriffsverwaltung

Der Anbieter muss die folgenden Anforderungen umsetzen, um sicherzustellen, dass nur autorisierte Benutzer Zugang zu Informationen erhalten, die für die Leistungserbringung gegenüber RWE relevant sind.

Identifizierung

- **An- und Abmeldung von Benutzern** Der Anbieter sollte über geeignete Verfahren zur Erstellung und Löschung von Benutzerkonten verfügen. Dazu gehören auch entsprechende Genehmigungen durch RWE, wenn neue Benutzerkonten eingerichtet werden sollen, die für die Leistungserbringung gegenüber RWE relevant sind. Der Anbieter muss den Abmeldeprozess regelmäßig überprüfen und in der Lage sein, auf Anfrage von RWE einen aktuellen Stand der verwendeten Zugangskonten des Anbieters, die für die Leistungserbringung gegenüber RWE relevant sind, vorzulegen.
- **Eindeutige Verwendung von Benutzer-IDs**: Benutzer-IDs werden im Verhältnis Eins-zu-Eins vergeben; jede Person erhält ein personalisiertes Benutzerkonto und ist auf dieses Konto beschränkt.
- **Überprüfungen des Benutzerzugangs:** Alle gewährten Zugangsrechte werden vom Anbieter regelmäßig überprüft.

Authentifizierung

- Für den Zugang zu den Ressourcen muss jede Person authentifiziert werden, um ihre Identität und ihre Verantwortlichkeit für die in den Systemen durchgeführten Aktionen zu bestätigen.
- In Anbetracht der Tatsache, dass Passwörter als primärer Authentifizierungsmechanismus für den Zugriff auf IT-Ressourcen von RWE verwendet werden, müssen die im Kapitel 4.6.11 Passwortmanagement definierten Anforderungen erfüllt werden.
- Die Benutzerauthentifizierung muss immer dann eingesetzt werden, wenn sie vom System unterstützt wird, so dass die Benutzeranmeldedaten nur einmal angegeben werden und Passwörter und/oder PINs nicht erraten werden können. Die Benutzer müssen aufgefordert werden, sie nach der ersten Nutzung zu ändern.
- Je nach Art und Sensibilität der Informationen/Systeme sollten zusätzliche Authentifizierungsfaktoren (Multi-Faktor-Authentifizierung, MFA) eingeführt werden, um

den Zugang zu den Systemen weiter abzusichern (z. B. mithilfe von Tokens, Chipkarten, biometrischen Merkmalen).

Berechtigung

- Der Anbieter erkennt an, dass RWE ihm Zugang zu sensiblen Informationen gewähren kann, und erklärt sich damit einverstanden, dass der gewährte Zugang ausschließlich für die Zwecke der vertraglichen Vereinbarung genutzt wird. Der Anbieter wird eingeräumte Zugangsrechte nicht dazu nutzen, sich Zugang zu Informationen zu verschaffen, die nicht ausdrücklich von RWE freigegeben wurden und somit zur Erfüllung der vertraglichen Vereinbarung nicht erforderlich sind.
- Der Anbieter muss den Zugang zu den Informationen entsprechend der jeweiligen Vertraulichkeitsstufe schützen. Siehe auch das Kapitel „Klassifizierung der Schutzbedürftigkeit von Informationen“ in diesem Dokument.

4.6.11 Passwortmanagement

Der Anbieter muss strenge Passwortanforderungen für alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung gegenüber RWE relevant sind, festlegen, um sensible Informationen zu schützen und den unbefugten Zugang zu Systemen und Daten zu verhindern. Starke Passwörter sind ein entscheidender Schutz gegen Cyber-Bedrohungen wie Hacking, Phishing und Malware-Angriffe.

- Sämtliche Konten müssen mit (änderbaren) sicheren Passwörtern geschützt sein. Eine Passwortrichtlinie sollte festgelegt werden, damit mindestens die folgenden Anforderungen erfüllt werden:
    - Mindestlänge des Passworts (z.B. 12 Zeichen)
    - Anforderungen an die Komplexität (z.B. keine Wörter aus dem Wörterbuch, Verwendung einer Mischung aus Buchstaben und Zahlen, Verwendung von Sonderzeichen usw.)
    - keine Wiederverwendung von Passwörtern (z.B. Passwortverlauf)
    - Verschlüsselung von Passwörtern bei der Übertragung oder Speicherung
    - Versand von Passwörtern getrennt von Kontoinformationen, um die Vertraulichkeit der Informationen zu gewährleisten
- Je nach Art und Kritikalität der Leistung und den Sicherheits-/Schutzanforderungen muss eine Multifaktor-Authentifizierung durchgeführt werden.

4.6.12 Back-up und Wiederherstellung

Um zu verhindern, dass Daten verloren gehen, muss der Anbieter sicherstellen, dass für alle Systeme, Anwendungen, Netzwerk-, Infrastruktur- und Endgeräte, die für die Leistungserbringung

gegenüber RWE relevant sind, Back-up-Prozesse umgesetzt werden (entsprechend der jeweiligen Schutzanforderungen).

- Der Anbieter muss sicherstellen, dass die Anforderungen an die Back-up-Speicherung, die Ausführungshäufigkeit und den Schutz vor unberechtigtem Zugriff in Bezug auf den Schutzbedarf der für RWE erbrachten Leistungen erfüllt werden.
- Die implementierten Prozesse zur Sicherung und Wiederherstellung müssen regelmäßig getestet werden, d. h. anhand regelmäßiger Tests der Sicherungsmedien, um sicherzustellen, dass sie im Notfall zuverlässig sind.

4.6.13 Business Continuity und Disaster Recovery

Um die Auswirkungen von Prozessunterbrechungen im Rahmen der Leistungserbringung gegenüber RWE zu minimieren, sollte der Anbieter über ein Disaster-Recovery-Programm (DR-Programm) oder eine Business-Continuity-Management (BCM) verfügen.

- Diese müssen so gestaltet sein, dass ein Datenverlust verhindert wird und der Anbieter auch im Falle einer Betriebsunterbrechung weiterarbeiten und die in seinem Vertrag mit RWE festgelegten Leistungen erbringen kann.
- Die für RWE erbrachten Dienstleistungen sollten durch einen Plan für die Betriebskontinuität (BCP) abgedeckt werden. Für die damit verbundenen Anlagen muss es einen Disaster-Recovery-Plan (DR-Plan) geben. Der Anbieter muss sicherstellen, dass der Geltungsbereich des BCP und des DRP alle Standorte, beteiligten Mitarbeiter und Informationssysteme umfasst, die zur Leistungserbringung gegenüber RWE eingesetzt werden.
- Der BCP und der DRP müssen regelmäßig gepflegt und getestet werden.
- Die Dokumentation über den Umfang und das Ergebnis der Prüfungen ist RWE auf Anfrage vorzulegen.

4.6.14 Cloud-Sicherheit

Der folgende Abschnitt betrifft ausschließlich Anbieter, die Cloud-Umgebungen bereitstellen oder nutzen, die für die Leistungserbringung gegenüber RWE relevant sind:

- Auf die Nutzung von Cloud-Umgebungen zur Leistungserbringung gegenüber RWE muss hingewiesen werden.
- In Abhängigkeit von den Anforderungen an die Informationssicherheit müssen in der Cloud-Umgebung geeignete (dem Stand der Technik entsprechende) Sicherheitsmaßnahmen getroffen werden.

- Die Sicherheitsmaßnahmen müssen über den gesamten Lebenszyklus der Cloud-Umgebung hinweg angewendet werden.

4.7 Compliance und Bewertungen

- Auf Anfrage muss der Anbieter einen von RWE (oder einem von RWE beauftragten Dritten) ausgestellten Sicherheitsfragebogen beantworten und eine schriftliche Antwort (einschließlich entsprechender Nachweise) vorlegen, damit RWE die Einhaltung der Anforderungen dieser Richtlinie beurteilen kann.
- Damit RWE die Einhaltung der Anforderungen dieser Richtlinie bestätigen/gewährleisten kann, ist RWE (oder ein von RWE beauftragter Dritter) berechtigt, auch Vor-Ort-Bewertungen in allen relevanten Räumlichkeiten des Anbieters durchzuführen. Der konkrete Umfang, die Dauer und die Organisation der Sicherheitsbewertungen vor Ort werden mit dem Anbieter nach angemessener Vorankündigung abgesprochen und abgestimmt.
- Der Anbieter stellt die Unterstützung der benannten Vertreter von RWE, die an solchen Sicherheitsbewertungen vor Ort beteiligt sind, und die Zusammenarbeit mit diesen Vertretern sicher. Diese Unterstützung umfasst den Zugang zu allen relevanten physischen Räumlichkeiten, Systemen und Mitarbeitern sowie die Bereitstellung relevanter Dokumente, zu denen unter anderem Prozessdokumentationen, (Sicherheits-)Richtlinien und Leitlinien sowie sicherheitsbezogene Leistungsüberwachungsberichte gehören. Darüber hinaus muss der Anbieter seine Auftragnehmer und Unterauftragnehmer dazu verpflichten, diesen Verpflichtungen in gleicher Weise nachzukommen.
- Im Falle von Schwachstellen, Abweichungen und/oder Nichtkonformitäten, die während des (dokumentierten) Prozesses der Selbstauskunft zur Sicherheit und/oder im Rahmen der Sicherheitsbewertungen vor Ort festgestellt werden, stellt der Anbieter sicher, dass geeignete Pläne zur Risikominderung und Abhilfemaßnahmen zeitnah umgesetzt werden. Die Ergebnisse werden RWE mitgeteilt.

5 Außer Kraft gesetzte Konzernregelungen

IT-Sicherheitsrichtlinie für den RWE-Konzern (V. 2.2, gültig ab 20.06.2008 einschließlich Anhang 1: Mindeststandard der IT-Sicherheit für IT-Benutzer sowie Anhang 2: Mindeststandard der IT-Sicherheit für den IT-Dienstleister)

6 Anhänge

6.1 Anhang 1: Klassifizierung und Kennzeichnung von Informationen

Wie Schutzmaßnahmen aussehen, hängt davon ab, wie umfassend Informationen geschützt werden müssen. Dieses Schutzniveau ist unabhängig von dem Medium, auf dem die Informationen vorliegen (analog oder digital).

Zu diesem Zweck teilt RWE Informationen in drei Vertraulichkeitsklassen ein, die sich nach den Auswirkungen eines möglichen Schadens richten:

Intern	Die Folgeschäden können begrenzt und überschaubar sein (z. B. interne Richtlinien, Prozessbeschreibungen; personenbezogene Daten, die allgemein zur Erfüllung von Geschäftsaufgaben benötigt werden, z. B. Adressbücher).
Vertraulich	Die Folgeschäden können beträchtlich sein (z. B. vorzeitige Veröffentlichung von Projektplänen, Veröffentlichung von Vertragsunterlagen; personenbezogene Daten, deren Verlust, Beschädigung, Weitergabe oder unrechtmäßige Verarbeitung dem Betroffenen erheblichen Schaden zufügen kann, z. B. Bankdaten).
Streng vertraulich	Die Folgeschäden können katastrophal sein und die Existenz des Unternehmens bedrohen (z. B. Entscheidungen über beabsichtigte Unternehmenskäufe/-verkäufe, Geschäftsgeheimnisse; personenbezogene Daten, die Auskunft über Gesundheit, Sexualleben, ethnische Herkunft, politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit und genetische/biometrische Daten geben).

Im Folgenden werden Informationen der Schutzklassen „vertraulich“ und „streng vertraulich“ zusammenfassend als „sensible Informationen“ bezeichnet.

Der Informationseigentümer legt die Klassifizierung für seine Informationen zu Beginn des Lebenszyklus fest (z. B. anhand der Kriterien in **Tabelle1:Klassifizierung** der Schutzbedürftigkeit von Informationen).

- Hat der ursprüngliche Informationseigentümer keine Einstufung vorgenommen, muss der (nächste) Informationseigentümer die Klassifizierung vornehmen, nachdem die Informationen übertragen worden sind.
- Bei sensiblen Informationen muss der Eigentümer der Informationen eindeutig aus dem Dokument ersichtlich sein.
- Bitte beachten Sie, dass sich die Notwendigkeit des Schutzes von Informationen im Laufe der Zeit ändern kann.

Kennzeichnung von Informationen anhand von Vertraulichkeitsklassen

- Informationen müssen mit einer Vertraulichkeitsklasse gekennzeichnet sein. Verwenden Sie immer nur die höchste anwendbare Klassifizierung.

Intern	- Die Dokumente sollten auf der ersten Seite gekennzeichnet werden.
Vertraulich	- Die Dokumente müssen auf jeder Seite gekennzeichnet werden. - Datenträger/Umschläge müssen gekennzeichnet werden.
Streng vertraulich	- Die Dokumente müssen auf jeder Seite gekennzeichnet werden. - Datenträger/Umschläge müssen gekennzeichnet werden.

- **„Öffentliche“** Informationen nehmen eine besondere Rolle ein. Sie müssen nicht gekennzeichnet werden, aber sie müssen von den autorisierten Geschäftsfunktionen (z. B. Corporate Communications) klassifiziert und veröffentlicht werden.
- Informationen ohne sichtbare Kennzeichnung können als **„Intern“** betrachtet werden, sofern es sich dabei nicht um offensichtlich sensible Informationen handelt. Dies gilt nicht, wenn die Informationen offensichtlich **„öffentlich“** sind (z. B. Werbebroschüren).
- Eine Anpassung der Kennzeichnung darf nur nach Rücksprache mit dem Informationseigentümer vorgenommen werden.

  Der Informationseigentümer muss die Klassifizierung anpassen, wenn sich der Schutzbedarf ändert.

Hinweis:

- Dokumente mit der niedrigsten Schutzklasse werden als „Intern“ gekennzeichnet. Diese Kennzeichnung bedeutet, dass diese Informationen ohne Einschränkung an RWE-Mitarbeiter weitergegeben werden dürfen. Diese Dokumente sollten jedoch nur im Bedarfsfall an externe Stellen weitergegeben werden.
- Pro Dokument wird nur eine Kennzeichnung vergeben. Es ist die jeweils höchste Kennzeichnung zu verwenden. Ein Dokument kann also nicht als „intern vertraulich“ gekennzeichnet werden.

6.1.1 Klassifizierung der Schutzbedürftigkeit von Informationen

Klassifizierung	Öffentlich (Public) (Öffentlich)	Intern (Intern)	Vertraulich (Vertraulich)	Streng vertraulich (Streng vertraulich)
Schutzbedarf	Kein Schutzbedarf	Gering bis mittel	Hoch	Sehr hoch
Mögliche Auswirkungen	Keine.	– Sehr geringe Auswirkungen auf RWE, seine Mitarbeiter sowie seine Kunden und Geschäftspartner.	– Verletzung von Persönlichkeitsrechten – Erhebliche Störung/Beendigung einer wichtigen Geschäftsbeziehung – Wichtige Aufgaben lassen sich nur eingeschränkt erledigen.	– Massive Verletzung der Persönlichkeitsrechte, schwere Rufschädigung. – Erhebliche Störung/Beendigung einer wichtigen Geschäftsbeziehung mit Auswirkungen auf andere Geschäftsbeziehungen – Wichtige Aufgaben können nicht mehr ausgeführt werden.
Beispiele	– Produktinformationen – Pressemitteilungen – Externe Stellenausschreibungen – Namen und offizielle Kontaktdaten von Mitarbeitern mit Verbindungen zur Öffentlichkeit (z. B. Ansprechpartner für die Rekrutierung, Pressesprecher)	– Kommunikation innerhalb des RWE-Konzerns – Interne Richtlinien – Prozessbeschreibungen – Adressbücher – Organigramme – Personalnummer und R-UI	– Kundendaten – Betriebspläne – Sicherheitskonzept (z. B. für die Jahreshauptversammlung) – Unveröffentlichte Sicherheitsvorfälle – Persönliche Informationen über das Arbeitsverhältnis (z. B. Gehaltsdaten) – Bankdaten	– M&A-Projekte – Geschäftsentwicklungsprojekte – Geschäftsgeheimnisse – Konformitätsprobleme – Medizinische Daten – Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person – Daten zum Sexualleben oder zur sexuellen Orientierung – Strafrechtliche Verurteilungen und Straftaten

Klassifizierung	Öffentlich (Public) (Öffentlich)	Intern (Intern)	Vertraulich (Vertraulich)	Streng vertraulich (Streng vertraulich)
Geteilter Zugriff	Die Informationen in dieser Kategorie sind nicht eingeschränkt.	Informationen dieser Kategorie dürfen nur innerhalb des RWE-Konzerns und mit relevanten externen Geschäftspartnern geteilt werden.	Informationen dieser Kategorie dürfen nur den Stellen und/oder Mitarbeitern zur Verfügung gestellt werden, die diese Daten zur Erfüllung ihrer Aufgaben benötigen.	Informationen dieser Kategorie dürfen nicht an die Öffentlichkeit gelangen und dürfen nur nach dem Need-to-know-Grundsatz weitergegeben werden.
Kennzeichnung	Öffentliche Informationen müssen nicht gekennzeichnet werden, dürfen aber nur von den befugten Unternehmensfunktionen (Corporate Communications) klassifiziert und veröffentlicht werden.	Interne Informationen sollten auf dem Deckblatt mit dem Vermerk „Allgemeines“ gekennzeichnet werden.	Vertrauliche Informationen müssen auf jeder Seite oder auf jedem Teil der Informationen deutlich mit dem Vermerk „Vertraulich“ gekennzeichnet werden. Datenträger sind entsprechend zu kennzeichnen.	Streng vertrauliche Informationen müssen auf jeder Seite oder auf jedem Teil der Informationen deutlich mit dem Vermerk „Streng vertraulich“ gekennzeichnet werden.

Tabelle 1: *Klassifizierung der Schutzbedürftigkeit von Informationen*

6.2 Anhang 2: Begriffsbestimmungen

Begriffe	Erläuterung
Vertrag	Alle geltenden Vereinbarungen zwischen RWE und dem Anbieter, einschließlich des Vendor Services Agreement (Anbieter-Leistungsvertrag), des Master Service Agreement (Dienstleistungsrahmenvertrag), des Professional Services Subcontract Agreement (Unterauftrag über professionelle Dienstleistungen), des Supplier Base Agreement (Anbieter-Basisvertrag) und der geltenden Lizenz- und sonstigen Vereinbarungen, gemäß denen der Anbieter Leistungen erbringt
Vermögenswert (Asset)	Jeder materielle oder immaterielle Gegenstand im Eigentum von RWE, für den ein Anbieter verantwortlich ist
Authentifizierung	Der Schritt der Überprüfung der Identität, d. h. Benutzer, System
BSI	Bundesamt für Sicherheit in der Informationstechnik (deutsche Bundesbehörde, die für die Verwaltung der Computer- und Kommunikationssicherheit der deutschen Regierung zuständig ist)
Vertraulichkeit	Erhaltung genehmigter Zugangs- und Offenlegungsbeschränkungen, einschließlich Maßnahmen zum Schutz der Privatsphäre und geschützter Informationen
Kryptografischer Schlüssel	Eine Information in digitalisierter Form, die von einem Verschlüsselungsalgorithmus verwendet wird, um Klartext in Chiffretext umzuwandeln
CVSS	Bezieht sich auf das Common Vulnerability Scoring System (allgemeines Bewertungssystem für Schwachstellen)
ENISA	Agentur der Europäischen Union für Cybersicherheit
Einrichtungen	Gebäude, Ausrüstungsgegenstände oder Dienstleistungen, die für einen bestimmten Zweck bereitgestellt werden
FIPS	Federal Information Processing Standard (US-Standard für Informationsverarbeitung)

Integrität	Der Schutz vor unsachgemäßer Veränderung oder Zerstörung von Informationen und die Gewährleistung der Unleugbarkeit und Authentizität von Informationen
Partner	Jede mit RWE verbundene Organisation, die an einer gemeinsamen Aktivität teilnimmt oder ihre Ressourcen bündelt, um ein gemeinsames Ziel zu erreichen
Persönliche Informationen	Alle Daten, die sich auf eine identifizierte oder identifizierbare lebende Person beziehen; eine identifizierbare Person ist eine Person, die direkt oder indirekt durch Bezugnahme auf eine Identifikationsnummer oder auf einen oder mehrere Faktoren, die für ihre physische, physiologische, mentale, wirtschaftliche, kulturelle oder soziale Identität spezifisch sind, identifiziert werden kann.
Risikobewertung (Risk Assessment)	Ein Verfahren zur Ermittlung und Bewertung von Risiken und potenziellen Auswirkungen. Die Risikobewertung umfasst die Beurteilung der kritischen Funktionen, die für die Fortführung des Geschäftsbetriebs einer Organisation notwendig sind, die Festlegung der Kontrollen, die zur Verringerung der Gefährdung der Organisation eingesetzt werden, und die Bewertung der Kosten für diese Kontrollen. Bei der Risikoanalyse werden häufig die Wahrscheinlichkeiten des Eintretens bestimmter Ereignisse bewertet.
Rollenbasierter Zugang	Zuweisung von Benutzern zu Funktionen oder Titeln. Jede Funktion oder jeder Titel definiert eine bestimmte Berechtigungsstufe.
Sicherheitsvorfall	Definiert als ein Verstoß oder die unmittelbare Gefahr eines Verstoßes gegen Sicherheits- oder Nutzungsrichtlinien oder Standard-Sicherheitspraktiken
Sensible Informationen	Bezieht sich auf Daten, die vor unbefugtem Zugriff geschützt werden müssen, um die Privatsphäre oder Sicherheit einer Person oder Organisation zu gewährleisten
Dienstleistungen	Vom Anbieter für RWE auszuführende Arbeiten, die in einem Vertrag, einer Vereinbarung oder einer Arbeitsanweisung festgelegt sind

Anbieter	Bezieht sich auf die natürliche oder juristische Person, die RWE im Rahmen einer vertraglichen Vereinbarung ein Produkt oder eine Dienstleistung zur Verfügung stellt, unabhängig von der Organisationsform
Schwachstelle	Eine Schwachstelle in der Gestaltung, Umsetzung, dem Betrieb oder der internen Kontrolle eines Prozesses, wodurch das System Bedrohungen durch gefährliche Ereignisse ausgesetzt sein könnte

Tabelle2:Begriffsbestimmungen